DEVELOPING CONFIDENTIALITY PROTECTIONS FOR A COMPUTERIZED MEDICAL RECORD SYSTEM BETWEEN SITES

ensuring the privacy of patients whose clinical records are on public domain software

PREPARED BY

Barbara Blechner
Children's Health Network
Hartford Primary Care Consortium
30 Arbor Street North
Hartford, Connecticut 06106
(860) 233-7561

December 1997

U.S. Department of Health and Human Services
Public Health Service
Health Resources and Services Administration
Maternal and Child Health Bureau
Project # MCJ-097112

Table of Contents

Acknowledgements

The author wishes to thank the members of the Confidentiality Work Group for their time, insight, and information: L. Deutsch, A. Geertsma, J. Landwirth, E. Nievas, J. Solomon, and M.E. Whiteman. In addition, gratitude is extended to the members of the Children's Health Network Task Force: J. Bronzino, L. Clark, L. Deutsch, S. Farmer, P. Gionfriddo, and D. Olson for their understanding and insight; to the staff at Betances School and La Casa de Puerto Rico for their help in implementing the consent process; and to the Maternal and Child Health Bureau of the Health Resources and Services Administration, U.S. Public Health Service for their support. This project was supported by MCHB, Grant #MCJ-097112.

– Barbara Blechner, M.Ed., J.D.
Chairperson, Confidentiality Work Group
Children's Health Network Task Force

Summary

ISSUES Confidentiality is a basic element of the physician-patient relationship. While the computerization of medical records has many significant advantages, the computer and the information stored must be adequately protected to avoid problems related to confidentiality.

GOALS The Children's Health Network sought to protect the confidentiality of medical records in a new computerized system that would collect, store and transfer pediatric patient information among various health care sites. This system would help to improve the quality of care for children from underserved areas, who often see multiple providers at different sites.

FUNDING After receiving support from local individuals, institutions and agencies in the Hartford, Connecticut area, the Children's Health Network gained funding in 1993 as a Field Initiated Project, Special Programs of Regional and National Significance (SPRANS) grant, from the Maternal and Child Health Bureau (MCHB) of the Health Resources and Services Administration (HRSA), U.S. Public Health Service.

PROCESS A Confidentiality Work Group of the Children's Health Network, headed by a lawyer/ethicist, studied reports from health care and other national associations regarding collection and protection of patient information. The group also reviewed provisions in current federal and state law to determine the boundaries of confidentiality, with the assistance of students from the Health Law Clinic of the University of Connecticut School of Law.

PRODUCT To protect the confidentiality of computer-linked patient records, CHN determined that it would be necessary to:

A. Obtain parental consent to enter a child's medical information into the network

B. Develop a technologically advanced computer system with appropriate security safeguards built into the system.

C. Develop policies and procedures governing the use of the system network.

D. Educate and train staff about confidentiality and its importance in computer-based medical records.

Details about achieving these goals, as well as recommendations for further study, are presented in this report.

In 1991, two patient care sites in downtown Hartford, Connecticut, agreed to develop a shared computerized medical records system. To ensure that the principle of protecting confidentiality was incorporated into the design of the system, a work group of experts was convened. This paper will briefly describe the Children's Health Network and its proposed system, and then detail various provisions devised to protect patient confidentiality within the system.

1. Background

1a. Confidentiality

Since the time of the Hippocratic oath, physicians have sworn to keep confidential what they see or hear during the course of treatment.1 Confidentiality is said to be basic to health care—the cornerstone of the physician-patient relationship.2 When the patient trusts that the physician will not reveal the content of a private conversation, the patient can feel free to discuss the most intimate of problems honestly and without fear of disclosure. As a result, the physician can gather all necessary information and then provide the needed services and appropriate care. Often, the medical record includes sensitive and confidential information about the most private aspects of a patient's life. The patient who is willing to disclose such information expects that the physician will not re-disclose the information without the patient's consent.

New technical capabilities including computerization of the patient medical record are extremely beneficial. Advantages include improvement of quality of patient care, linkages to outside sources for guidelines and decision support during the patient encounter, and value to secondary data repositories and registries. See the companion paper, "Computer-Based Patient Records for Pediatric Primary Care and Public Health: Modernizing Clinical Information Systems with Public Domain Software," for a full description of the Children's Health Network's effort to develop and provide public domain, computer-based patient record systems, particularly to underserved areas and smaller institutions that lack internal means.3

While the computerization of medical records has many significant advantages, it has also created some challenging problems related to confidentiality. Although paper records can be

locked up, computer records are readily accessed throughout a hospital or clinic. Even outside computers, such as those from office practices, may be part of the system. Electronic storage of medical information thereby allows for easy access to sensitive data if the computer and the information stored in it are not adequately protected.4

Various federal and state laws impose an obligation on health care providers to preserve the confidentiality of medical records in specific situations, although these laws do have limitations. Courts have recognized a legal duty to maintain the confidentiality of medical records. Legal relief has been granted by the court system under a number of theories, including
negligence, breach of implied contract and invasion of privacy.5 The Privacy Act of 1974 manifests specific requirements for a record-keeping organization to establish reasonable and proper information management policies and practices. These requirements are intended to assure that the collection, maintenance, use and dissemination of information is necessary, lawful, current and accurate.6 Recently enacted federal legislation directs the Department of Health and Human Services to develop regulations to protect medical records.7

In addition, professional organizations have established principles and guidelines about confidentiality. The Association of American Medical Colleges, for example, supports the principle that individuals have the right to expect their identified health and medical information not to be disclosed without their express consent. This concept has established a standard of care within the profession that imposes a duty upon health care providers to protect the confidentiality of patients' medical information.

However, patients should be aware that information about their medical conditions is stored in computers that are accessible to people other than their own physicians.8

1b. Children's Health Network (CHN)

In an effort to improve pediatric health care in downtown Hartford, a group of health care providers proposed the establishment of a city-wide, multi-institutional consortium in the spring of 1991. Providers had long been concerned that, because many pediatric patients

sought care from multiple providers and sites, complete medical record information was not always available at a given site. The goal of the consortium was to develop a system that would electronically collect, store and transfer medical and demographic data on pediatric patients in Hartford. Such a system would help to improve the quality of children's primary care through a computerized, linked clinical information system that could be accessed by participating health care providers. Members of the proposed network would include community health centers, hospital ambulatory care units, emergency rooms and school-based clinics. While such a computerized system would have many advantages, reservations were expressed early on by participating institutions regarding confidentiality of patient medical records.

The confidentiality issues raised were taken seriously by those planning the system. In order to ensure that the proposed system was legally and ethically acceptable, the planners sought help from a health lawyer educator at the University of Connecticut Health Center. He suggested enlisting the assistance of a law student from the University of Connecticut School of Law's Health Law Clinic, which was held at the University of Connecticut Health Center. After reviewing the existing literature, the student indicated in a final report that although computerization of medical data is convenient, convenience alone is an insufficient reason to justify its use. The report further cautioned that computerization of personal data poses a unique threat to confidentiality and privacy, which clearly must be protected.9 While the report ultimately did recommend implementation of the proposed ambulatory care computer network for pediatric patients, it detailed protections that should be instituted in such a system. Recommendations included restricting access to the computer system and implementing a strict computer security plan.10

Under the name of the Children's Health Network (CHN) of the Hartford Primary Care Consortium (HPCC), a small, multi-disciplinary advisory group developed a plan to provide public domain, computer-based patient record systems to underserved areas. The plan was predicated on a commitment to protect the confidentiality of patients' medical records by every means reasonable. The group received funding as a Field Initiated Project, Special Programs of Regional and National Significance (SPRANS) grant from the Maternal Child Health Bureau

of the U.S. Department of Health and Human Services. On October 1, 1993, planning for a demonstration project began.

CHN proposed the establishment of a computer medical record link between an elementary school-based clinic in downtown Hartford and a large city hospital. Computer transfer of patient records between the Hartford Hospital Pediatric Ambulatory Care Clinic (HHPACC) and the school-based health center at Betances School was the initial goal of CHN.

Since privacy and confidentiality issues emerged as areas of great concern to CHN, an assistant professor in the Department of Community Medicine at the University of Connecticut School of Medicine was appointed to the planning committee. As a health lawyer, ethicist and educator teaching law and ethics, her focus was to ensure that confidentiality was protected to the greatest extent possible in the development of a model system. Questions arose immediately regarding the various stages of system development, including technical design, planning for implementation at each site, clinical information management and potential use of aggregate data at the state and national levels.11 It was recognized that the protection of confidentiality and privacy would be one of the most significant questions to be addressed in the design of the system. Consequently, a Confidentiality Work Group was formed, headed by the health lawyer/ethicist educator, to address the multitude of problems related to confidentiality.

1c. The Confidentiality Work Group

The Confidentiality Work Group's purpose was to establish reasonable precautions to protect the confidentiality of patient records. Specifically, the objectives were to: 1) balance patients' privacy rights and the confidentiality of identifiable patient information with legitimate data uses; 2) ensure the integrity, accuracy, consistency, reliability and validity of information contained in the patients' medical records; and 3) ensure that parents and legal guardians of pediatric patients are adequately informed of their right to privacy and confidentiality for their children's medical record information, their right to personal access to such information, their right to refuse transfer of information, their right to revoke consent to the transfer of

information, and limits placed on these rights as required by state or federal laws or regulations.12

Headed by the health lawyer/ethicist and the Confidentiality Work Group included: a nurse/attorney from a large law firm in Hartford (serving in a pro bono capacity); an attorney who, as litigation director of the Legal Aid Society, represented many of the interests of inner city pediatric patients; a physician/attorney who was Acting President and CEO of a children's hospital; and a community representative who was a parent from Betances School, the proposed school-based clinic site. The principal investigator of the project, a physician with training in public health, was also an active member of the group. Periodically, as needed, the group was enlarged to include physicians, nurses, state health workers, public school educators and administrators, and others interested in the project.

The Confidentiality Work Group studied reports from the American Association of Medical Records, the American Medical Association, the American Health Information Management Association, the Computerized Patient Records Institute (CPRI), the Institute of Medicine, and the Office of Technology Assessment, among others. This review of literature was part of the Group's effort to develop protocols for safeguarding patient privacy and confidentiality, and to keep data secure and complete. A bibliography of relevant journal articles, books, and reports is located in the Appendix.

2. Confidentiality provisions in the law

The first task of the Confidentiality Work Group was to review existing confidentiality provisions in current federal and state law, in order to determine the legally defined boundaries of confidentiality. Once again, assistance was sought from students in the Health Law Clinic of the University of Connecticut School of Law. The ensuing report indicated that legal protection of medical information suffers from lack of uniformity that results in administrative uncertainty and potential violation in some jurisdictions with weaker confidentiality requirements.13 Further, those statutes that exist are very narrow and generally do not apply to computerized medical records.

2a. Federal and state confidentiality provisions

Federal Protections include: the Freedom of Information Act of 1966; the Privacy Act of 1974; the Americans with Disabilities Act; special United States Code rules protecting the confidentiality of records of patients who seek treatment for drug or alcohol abuse at federally funded facilities; Medicare Conditions of Participation requiring hospitals to have procedures to ensure the confidentiality of patient records; and Constitutional Law.

State protections include specific statutes, constitutional law and common law. These vary from state to state. In Connecticut, CHN's base of operation, certain communications are, by statute, designated as confidential and privileged. In a civil action, a physician, surgeon or other health care provider cannot disclose patient communications without the patient's consent. The most comprehensive protection of patient communications has been applied to the psychiatrist-patient relationship. The Connecticut legislature has identified certain types of medical records which, because of their sensitive nature, require special confidentiality rules. Records pertaining to psychiatric treatment, AIDS and HIV, alcohol and drug abuse treatment, examinations and treatment by communicable disease control clinics, children conceived by artificial insemination donation, and birth defect information are protected. In addition, all state agencies must adopt procedures to safeguard the confidentiality of personal data under its control.

The Connecticut state legislature has also identified a number of areas in which the public interest in protecting individuals from abuse or exposure to certain diseases outweighs the patient's interest in confidentiality. For example, health care providers are required to report abuse and neglect of: children, the aged, mentally retarded persons and residents in nursing homes. Providers must also report certain communicable diseases and specific HIV-related information.

2b. Professional guidelines and credentialing standards

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) mandates that medical records be kept by hospitals and other organizations. These records must be documented accurately, adequately and in a timely fashion. They must be readily accessible and stored in a confidential and secure manner. Written consent of the patient is required if medical information is released to others.

The American Medical Association's (AMA) Code of Ethics has had a section requiring physicians to maintain confidentiality since the first Code of Ethics was created in 1847.14 In 1992, the AMA revised its Code of Ethics and added a detailed section regarding the confidentiality of computerized medical records. Section 5.07, entitled Confidentiality: Computers, outlines the purposes of confidentiality15 and also its limits.16 Eight guidelines to ensure the maintenance of proper confidentiality are proposed.17 The Code of Ethics of the American Nurses' Association describes the right to privacy as "an inalienable right."18 The Patient's Bill of Rights of the American Hospital Association states that patients have a right to expect that every communication and record pertaining to their treatment will be kept confidential.19

These ethical codes and guidelines have been construed by courts as standards to which a health care provider must conform.20 If health care providers fail to maintain a patient's confidentiality, their actions fall below the proper standard of conduct. Providers are liable for malpractice under this reasoning.

2c. Liability issues and implications for CHN

Although federal and state laws regarding confidentiality are inconsistent, it is possible for patients to recover damages for an improper disclosure of medical records based on various common law theories. These theories include: breach of contract; invasion of privacy; breach of fiduciary duty; libel and defamation; and malpractice. Of great concern to CHN was the area of liability, since the ethical codes mentioned above have been construed by courts as standards of care to which health care providers must conform. CHN was concerned about its responsibility to abide by the standard of care established by law and professional guidelines. This gave the Confidentiality Work Group another reason to attempt to incorporate appropriate protections into the CHN system.

3. Implementing Measures to Protect Confidentiality

The Confidentiality Work Group determined that in order to protect confidentiality and privacy in a linked computer system, it was necessary to:

a. obtain parental consent to enter a child's medical information into the network

b. develop a technologically advanced computer system with appropriate security safeguards built into the system

c. develop policies and procedures governing the use of the system

d. educate and train staff about confidentiality and its importance in computer-based medical records

3a. Obtaining parental consent to enter a child's medical information into the network

The concept of consent was critical to this project. In order to transfer pediatric patient information from site to site, the Work Group agreed that it was necessary to obtain parental consent to enter a child's medical information into the network. Traditionally, medical records have been viewed by the courts as the property of the institution or practitioner that create and maintain them.21 The medical record is, therefore, owned by the provider or facility that produced it. Nonetheless, medical records are subject to the patient's right or claim to in the recorded information.22 Patients have a legal right to the information, which belongs to them, and they may expressly consent or not to the release of medical information in their records. According to Harold Edgar and Hazel Sandomire in "Medical Privacy Issues in the Age of AIDS," "People have a primary interest in who knows medical information about them. Personal control over what aspects of self an individual shares with others, and in what detail, is an important contemporary value."23 Since the information entrusted to the physician or hospital actually belongs to the patient, he or she, as the owner, must give consent before that private information can be divulged. This concept is important, because individuals untrained in principles of confidentiality (computer technologists, for example) generally are unaware of the difference between ownership of information and ownership of the medical record itself.

Consequently, certain staff may not be knowledgeable about the need for patient consent or the importance of protecting confidentiality.

By definition, informed consent must be competent, voluntary and informed. Therefore, the competent adult parents or guardians sign the consent form, and signing must occur without duress. Further, during the consent process, the parents or guardians must be fully informed about what they are consenting to. The Work Group decided that the consent form for transfer of medical records should be effective for one year from the date of signing, and that this time period would begin at the start of the school's fall semester. To ensure that parents would have the opportunity to reconsider a decision, the form would be updated and re-signed annually. Consent could be revoked at any time.

Before drafting a consent form for the CHN program, group members reviewed a number of parental consent documents for transfer of medical records. The resulting CHN consent form (see Appendix 5C), contains an information sheet with a description of the program and the purpose for transferring medical information from one site to another. The form requests permission to share the information with the school clinic and the hospital. The program is described, as well as the purpose of the disclosure. The type of information to be disclosed is detailed and includes: immunization history; illnesses; and any HIV, psychiatric, or drug and alcohol-related history documented in the health record. The form specifies to whom the information will be disclosed. Further, the form states that HIV, psychiatric, and drug and alcohol-related information will not be given to anyone else without the parent's or guardian's consent. The form also states that CHN information will be available to the parent or guardian upon request, and that if the parent does not want information shared between the two sites, treatment will still be available at either site. Names and telephone numbers of personnel at both sites are listed in case of questions. There is a separate section for a parent or guardian signature indicating refusal to share medical information. In addition, the form includes a statement to the effect that all reasonable precautions will be taken to keep medical information confidential. Although,

ideally, the consent process is most effective when explained on a one-to-one basis, it was understood that that would not always be possible. Therefore, much care was taken to make the form as easy to read as possible. It was also translated into Spanish.

After the draft was complete, input was sought from many individuals to ensure that important issues were discussed in the consent form and could be understood by readers. The form was read and revised by the Work Group, the consultants, community members, school parents, physicians, other staff from Betances School and HHPACC, attorneys and board members from the Hartford Primary Care Consortium, the Betances School principal, as well as the attorney for the Hartford Board of Education. School parents and staff at La Casa de Puerto Rico helped with the Spanish translation. Ultimately, the final form was handed to parents at the time of school registration, along with other standard school materials. At registration the second year, when consent forms were handed out, parent volunteers were present to answer questions and explain the purpose and content of the consent form. CHN found this method of transmitting information to parents and guardians an important tool in obtaining meaningful informed consent.

CHN collected and monitored consent forms for almost three years. By the second year, 96 percent of those who filled out the form agreed to transfer information. CHN was able to reach 430 of the 600 school families to either fill out a consent form or to return it unsigned. Again, in the second year, when forms were sent out, in order to increase the number returned, CHN offered a pencil to everyone who returned their forms. No pressure was exerted to have the forms signed, and pencils were given to any child who returned a form, whether or not the form was signed. All details – from initial design of the consent form to the meticulously ensuring that the form was understood – were important for the effectiveness of the program.

Demographic and other data from patients' medical records at Betances School were entered into the CHN computer database demographics file for use by the Betances School Clinic at the Betances School. No information was transferred to HHPACC, however, until a consent

form was signed. The computer application was programmed so that medical information could not be transferred until a consent form was signed, and this fact was to be entered by a specially designated person. At this point, if information was requested by a HHPACC physician, it could be transferred from Betances to HHPACC for use by the specially designated physician, and the updated record send back to Betances for storage. Planned modifications to the computer system would allow a patient to give consent at HHPACC (if consent had not already been given at Betances), and then to transfer the information from Betances to HHPACC. This would require that consent forms be available at HHPACC and that the staff be trained to administer the forms.

3b. Developing a technologically advanced computer system with appropriate security safeguards built into the system

One of the primary interests of the Confidentiality Work Group was to develop a secure system. Lengthy discussions focused on how to safeguard information in the patient record from unauthorized disclosure, modification, destruction or erroneous entries, while developing an efficient, effective computer system. CHN's aim was to establish a secure system for health care providers that was easy to use and cost-effective. The Watcom and Microsoft Windows NT databases were the two programs selected to develop effective system security. With the aid of these databases, the following protective mechanisms were built into the system:

- Confidentiality Reminder. Upon entering the CHN database, the first screen was programmed to indicate that all information accessed is confidential

- Dedicated Point-to-Point Line. A dedicated point-to-point communication telephone line from Betances to HHPACC was installed. This meant that no one other than Betances School and HHPACC personnel were able to dial into the computer. A dedicated, point-to-point line with only one connection between client and host ensured maximum data security. However, while it was possible to achieve this connection between Betances School and Hartford Hospital, a dedicated line could not be arranged because HHPACC moved to the new Connecticut Children's Medical Center-Primary Care Clinic (CCMC-PCC). Alternate plans to improve security included implementing a call-back system in which the computer sending the patient information would be called back by the receiving computer for confirmation. Encryption was also considered as an option.

- Firewall System. A firewall system was installed in the computers to protect information at Betances School Clinic, so that it was not sent to HHPACC without a signed consent form.

- Protected Sign-On System. A protected sign-on system was devised in multiple levels. First, users log on to Windows for Workgroups. Next, they log on to the Windows NT network. Lastly, users log on to the Watcom CHN database application, using user identification names and a six digit password set by the administrator. Passwords are known only to the users, and are changed periodically.

- Audit Trail. An audit trail that reveals irregular access was an important element of the system, recording users, accesses and on-line activities. CHN built an audit system into its computer program, enabling the information security manager or computer administrator to identify individuals logging on to specific files and applications. Such a system for journaling all activities, including any changes made to the on-line data and the dates those changes occurred, is essential to securing a computerized medical record system.

- Screen Shut Off. Screens were programmed to turn on a screen saver after three minutes of unattended time, limiting the possibility that a passerby might view confidential information. The plan was to eventually have the screen shut off completely after three to five minutes of unattended time, so that a password would be necessary for re-entry.

- Control of Access According to Job Function. The system was equipped with user-specific menus to control access to functions. This capability limits user access only to those parts of the medical record relevant to a given user's job function. For example, personnel registering patients into the system do not need access to information about mental illness. Additionally, CHN instituted multi-level security access, authorizing certain personnel to utilize the database for reading only, while others were permitted to read and enter data. Finally, a select few were authorized to read, enter and delete information if, for example, changes were necessary due to erroneous entries.

3c. Developing policies and procedures governing the use of the system

After rigorous efforts, the Work Group developed a policy and procedures document that addressed aspects of privacy, legal responsibility, data security, equipment security, data integrity and research requests (see Appendix 5.4). The Work Group determined that to be most effective, policies and procedures should be designed by the participating institutions.

Each facility would be responsible for establishing its own implementation and enforcement methods. Accordingly, CHN designed a series of suggested policies and procedures to protect confidentiality that facilities could use as a model in fashioning their own plans. The sample recommendations in the Appendix include information about CHN's experience, as well as specific to each policy. Those recommendations include the following provisions:

- Physical security of the computers is critical to protecting confidential information. Facilities must ensure that the computers are placed in secure locations where they cannot be easily accessed by passersby, particularly at night or on weekends. Ideally, computers should be in a locked space, or at least well protected from access. At Betances School, keyboards were removed each night and locked in a secure area. Finally, it was recommended that computers be situated so that patients and others cannot view the screens. If this is not possible, a barrier should be installed.

- Quality control for information input and updating. CHN developed a structured system of quality checks to ensure accuracy in transferring information from the medical record to the computer. Initial computer entries of student information at Betances School were checked for accuracy. Follow-up checks were conducted for every second, fourth, eighth and selected subsequent entries. Following the initial accuracy checks, a quality assurance check was conducted, first weekly and then monthly. Lastly, at the end of the second year, CHN checked a random sample of all data entries to ensure accuracy. All of these steps are necessary periodically to assure the integrity of data in the medical record.

- Passwords. Authorized personnel are given unique passwords by the computer administrator to avoid use of passwords that may be familiar and easily obtained by others (e.g., a birth date or telephone number). Passwords are composed of both letters and numbers, at least six digits in length, and are automatically changed every 60-90 days. Personnel must memorize their passwords and are cautioned not to write them down. If passwords are not used for a certain period of time, they are canceled. When authorized personnel terminate employment, their passwords and user ID numbers are immediately deactivated. Recommendations are that individuals not use passwords that are familiar, such as telephone numbers or birth dates. Passwords are not to be shared or disclosed to others, and sanctions are suggested if this rule is violated.

- Sign-off requirements. Authorized personnel must log-off the computer whenever they finish using it. Again, sanctions are suggested if this procedure is violated.

- User Access and Confidentiality Agreement. CHN developed a form for employees using the computers. The form includes the provision that personnel with access to the computers will

not disclose identifiable information without a specifically authorized consent form. Such an agreement documents the employee's responsibility to safeguard information. Although this kind of agreement has limitations, it does serve as a reminder—along with staff education programs—of the sensitivity of health care data and the obligation of health care personnel to preserve confidentiality and security of patient information. The confidentiality agreement developed by CHN (see Appendix 5.1) states that: 1) the network contains confidential medical information; 2) health care data may be obtained only for the reason it was originally provided; and 3) the employee has read and will conform to the policies and procedures regarding use of the computer system. In addition, the employee agrees not to disclose without informed consent any identifiable information to any individual or agency. The agreement further requires the employee to protect and not disclose the user log-on and password. Two final provisions of the confidentiality agreement refer to keeping the computer hardware and software secure, and signing off the screen when finished. CHN developed only one user access and confidentiality agreement form. However, others can be designed for personnel who are not employees of the facility, but have access to confidential information that is the property of the health care facility. These statements of responsibility and confidentiality should be signed by all new employees, and updated annually for all other authorized personnel.

- Audit System. An audit trail to uncover irregular or questionable access activity, as mentioned above, is an important element of the system. Users' accesses and on-line activities are recorded, allowing the information security manager to monitor the computer audit system on a regular basis. Other important issues that might be addressed in a policy, but are not included in the CHN sample document, are:
1) procedures and information about a backup system for duplicating information;
2) a system of independent audits to check user access; 3) procedures to verify that requests for information are valid; 4) specific functions of an information security manager; 5) procedures for patients to revoke, review and/or correct existing data; and 6) a process for implementing these policies and procedures in the facility, and for applying sanctions when breaches of security and confidentiality occur.

3d. Educating and training staff about confidentiality and its importance in computer-based medical records

In order to increase the staff's awareness of security needs, improve their security practices and, ultimately, protect the confidentiality of patient medical records, a staff education program is essential. Sessions should include: 1) a discussion of the rationale for confidentiality, including the pertinent legal and ethical issues; 2) the facility's current policies and procedures for protecting confidentiality; and 3) the specific responsibilities of individual

staff members. Training should be repeated annually.

4. Conclusions, recommendations, policy implications

Early in the project, CHN recognized its obligation to patients whose medical records were part of the network. The goal was to develop a system that was protective of patient confidentiality, yet easy to use. To achieve this goal, CHN's strategies included: 1) obtaining informed consent from the parents or guardians of the pediatric patients at the Betances School Clinic; 2) developing a computer system that built in strategic security mechanisms to protect data; 3) developing policies and procedures to assist facilities in implementing protective provisions; and 4) planning for staff educational programs regarding important confidentiality issues.

There were several areas of confidentiality protection that the group considered including in the project, but could not address within the given time period.

One suggestion involved assigning each patient a unique identifier or number that only the physician and patient would know. The identifier would not be linked in the data system to a particular person. However, such a system would require that patients always have their numbers, and that a master list of names and numbers be protected, but accessible when needed. These complexities may make this arrangement difficult for health care providers to use.

A second potential strategy for protecting confidentiality involved establishing separate computer screens for particularly sensitive information related to HIV, genetic, alcohol, drug and mental health records. Experts have said that the battle to protect general information may have been lost, but vigilant efforts must continue to protect this kind of highly sensitive information. Separate screens could be helpful. Lastly, the Work Group agreed that systems to protect confidentiality must also include policies and procedures to protect data utilized for research and public health purposes.

There is no foolproof method to assure protection of confidentiality. However, computer users must take their responsibility seriously. All of the precautions mentioned above, and others not described here, still cannot guarantee that someone will not be careless, or utilize the

computerized medical record for uses for which it was not intended, or that someone from outside the system will not intrude. It is imperative that primary care facilities make every effort to maintain the confidentiality of medical records. Perhaps what is necessary, in addition, is supportive federal law that demands confidentiality protection, establishes high standards of appropriate behavior for everyone handling medical records, and imposes significant penalties for breaches of confidentiality.

5.1. References

1. Furrow BR, Greaney TL, Johnson SH, Jost TS, Schwartz RS. Health Law, West Publishing Co., St. Paul, Minn., 1995.
2. Parsi KP, Winslade WJ, Corcoran K. Does confidentiality have a future? The computer-based patient record and managed mental health care. Trends in Health Care, Law & Ethics 10(1-2):78-82, 1995.
3. Deutsch L, Children's Health Network Technical Brief, Computer-based Patient Records for Pediatric Primary Care and Public Health: Modernizing Clinical Information Systems with Public Domain Software. Office of Systems, Education, and Analysis, MCHB, 1997.
4. Institute of Medicine. Health Data in the Information Age: Use, Disclosure, and Privacy, National Academy Press, Washington D.C., 1994. U.S. Congress, Office of Technology Assessment. Protecting Privacy in Computerized Medical Information, OTA-TCT-576. U.S. Government Printing Office, Washington, D.C., September 1993.
5. Institute of Medicine. Health Data in the Information Age: Use, Disclosure, and Privacy, National Academy Press, Washington D.C., 1994.
6. Ibid.
7. 42 U.S.C. §§ 1301 et. seq., Health Insurance Portability and Accountability Act of 1996, amending Title XI.
8. Siegler M. Confidentiality in Medicine - A Decrepit Concept. N. Engl. J. Med. 307:1518-1521, 1982.
9. Palumbo P. Community-Wide Information Network for Ambulatory Care. Prepared for University of Connecticut School of Law Health Law Clinic. May, 1991.
10. Ibid.
11. Rauh VA. Process Evaluation of the Children's Health Network Planning, Implementation, and Early Operations. Submitted to the Hartford Primary Care Consortium. June 20, 1996.
12. Ibid.
13. Rowen C. Computerized Medical Records and Confidentiality. Prepared for University of Connecticut School of Law Health Law Clinic. April 28, 1993.
14. AMA Code of Ethics 1847, Chap. I, Art. I, Subsection 9.
15. See supra, note 12.
16. Ibid.
17. AMA Principles of Medical Ethics 1992.
18. American Nurse's Association Code of Ethics, Point 2 (1976).
19. American Hospital Association, A Patient's Bill of Rights (1973).
20. See supra, note 12.
21. See supra, note 1. Southwick AF. The Law of Hospital and Health Care Administration. Health Administration Press, Ann Arbor, Michigan, 1988.
22. Roach WH, et. al. Medical Records and the Law. 2ed. Aspen Publishers, Inc., Gaithersburg, Maryland, 1994.
23. Edgar H, Sandomire H. Medical Privacy Issues in the Age of AIDS. American Journal of Law & Medicine XVI(1-2):155-222, 1990.

5.2. Bibliography

JOURNALS

Alpert S. Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform. Hastings Center Report, November/December 1993, pp. 13-23

American Medical Association Council on Ethical and Judicial Affairs. Code of Medical Ethics: Current Opinions with Annotations, Section 5.07, Confidentiality: Computers, pp. 82-83, 1996 Edition

Annas G. Privacy Rules for DNA Databanks: Protecting Coded 'Future Diaries.' JAMA, 270(19):2346-50, November 17, 1993

Barrows R. and Clayton P. Privacy, Confidentiality, and Electronic Medical Records. Journal of the American Medical Information Association , 3(2):139-48, March/April 1996

de Gorgey A. The Advent of DNA Databanks: Implications for Information Privacy. American Journal of Law & Medicine, 16(3):391-8

Gostin L., Turek-Brezina J., Powers M., et al. Privacy and Security of Personal Information in a New Health Care System. JAMA, 270(20):2487-93, November 24, 1997

McCarthy C. and Porter J. Confidentiality: The Protection of Personal Data in Epidemiological and Clinical Research Trials. Law, Medicine & Health Care, 19(3):238-41, Fall-Winter 1991

Milbolland D. Privacy and Confidentiality of Patient Information: Challenges for Nursing. JONA, 24(2):19-24, February 1994

Parski K., Winslade W., and Corcoran K. Does Confidentiality Have a Future? The Computer-Based Patient Record and Managed Mental Health Care. Trends in Health Care, Law & Ethics, 10(1/2):78-82, Winter/Spring 1995

Shapiro R. and Annas G. Who Sees Your Medical Records? Human Rights, Summer 1994

Siegler M. Confidentiality in Medicine—A Decrepit Concept. Sounding Board, NEJM, 307:1518-21, December 9, 1982

Winslade W. Confidentiality of Medical Records: An Overview of Concepts and Legal Policies. The Journal of Legal Medicine, 3:497-533, November 4, 1982

BOOKS AND REPORTS

Boston University School of Public Health, School of Medicine, Health Law Department, Health Care Records: Privacy and Confidentiality in the New Information Age, proceedings from 6th Annual Health Law and Bioethics Conference, November 17, 1995, Boston, Massachusetts

CPRI Work Group on Confidentiality, Privacy, and Security, "Guidelines for Establishing Information Security Policies at Organizations using Computer-based Patient Record Systems," Computer-based Patient Record Institute, 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173-4742, February 1995

CPRI Work Group on Confidentiality, Privacy, and Security, "Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems," Computer-based Patient Record Institute, 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173-4742, June 1995

CPRI Work Group on Confidentiality, Privacy, and Security, "Guidelines for Managing Information Security Programs at Organizations using Computer-based Patient Records," Computer-based Patient Record Institute, 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173-4742, January 1996

CPRI Work Group on Confidentiality, Privacy, and Security, "Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient Record Systems," Computer-based Patient Record Institute, 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173-4742, May 1996

Institute of Medicine, Division of Health Care Services, Committee on Regional Health Data Networks, Donaldson, Molla S. and Lohr, Kathleen N. (eds.), Health Data in the Information Age: Use, Disclosure, and Privacy, National Academy Press, Washington, DC 1994

Kunitz and Associates, Inc., "Final Report of the Task Force on the Privacy of Private-Sector Health Records," Contract HHS-100-91-0036, Kunitz and Associates, Inc., 6001 Montrose Road, Suite 920, Rockville, MD 20852, September 1995

Legal Action Center of the City of New York, Inc., Confidentiality: A Guide to the Federal Law and Regulations, Legal Action Center of the City of New York, New York, NY, 1995

National Research Council, For the Record: Protecting Electronic Health Information, National Academy Press, Washington, DC (in press). Prepublication copy of the book is available on-line at http://www.nap.edu

Roach, Jr., William H. and The Aspen Law Center, Medical Records and the Law (2ed.), Aspen Publishers, Inc. Gaithersburg, MD, 1994

System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Computers at Risk: Safe Computing in the Information Age, National Academy Press, Washington, DC, 1991

U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576, U.S. Government Printing Office, Washington, DC, September 1993

5.3. Sample Form

This sample form should not be used without the advice of the user's legal counsel.

CHILDREN'S HEALTH NETWORK
INFORMATION SHEET AND CONSENT FORM

The Children's Health Network is designing a computer system that will link all the places you may take your children for medical care. The system will make sure that the doctors and nurses have all the information they need to give your children good treatment. The computers will have medical information on children whose parents have agreed to be part of this system.

Right now, the Children's Health Network is starting with the Betances School Clinic and the Hartford Hospital Pediatric Ambulatory Care Clinic (HHPACC). No other places where you might take your children are part of the system yet. If you agree to be in the Network, information will only be shared by these two places.

The Betances School Clinic and HHPACC are trying to make sure that your child has year-round medical care. By using the computer system, the Betances School Clinic and HHPACC will be able to share information on the care your child has received at either place. For example, when the system is fully working if your child goes to HHPACC on the weekend, the Betances School Clinic will receive this information and be able to make sure your child is doing well when he or she gets to school.

It is up to you whether your child is part of the Children's Health Network. If you decide you do not want your child to be in the Network, you still will be able to get medical treatment at the Betances School Clinic and HHPACC. The attached consent form will give you more information about your rights.

(Please note: this document has also been translated into Spanish.)

Consent for Sharing Medical Information between Betances School Partnership and Hartford Hospital Pediatric Ambulatory Care Clinic (HHPACC)

With your permission, your child's health information will be put on a computer that will share the information only between Betances School Clinic and HHPACC. The reason for this computer record is to quickly give the health care providers at the school and the medical center information needed to provide good medical care to your child at any time that he or she goes to the school clinic or HHPACC.

The medical information that will be put on the computer can include immunization information, information about illness, and any HIV, psychiatric, and drug and alcohol-related information in the health record. The release of your identity and your child's identity will be limited to health care workers at the Betances School Clinic and HHPACC. HIV, psychiatric, and drug and alcohol-related information will not be given to anyone else without your special written consent or as required under Connecticut and Federal law. All reasonable precautions will be taken to keep your child's medical information confidential.

All Children's Health Network information about your child will be available to you upon request. Consent is up to you. If you do not want to share medical information between the Betances School Clinic and the HHPACC, your child can still get treatment at either place. This consent is good for one year, and can be revoked at any time by giving written, dated notice to Betances School Clinic.

Please sign only one of the areas below.

Agreement to Share Medical Information

I,_____, do give permission for my child, _____ to have health information put on a computer system designed by Children's Health Network. I understand that by doing so, my child's medical information, including HIV, psychiatric, drug and alcohol-related information, will be shared between the Betances School Clinic and HHPACC. I understand that all reasonable precautions will be taken to keep my child's medical information confidential. I have read and understand all of the information written on this sheet of paper. If I have any questions I can call the Betances personnel at 525-4640; or the Primary Care Center Coordinator at HHPACC.

Date: Signature_____
Parent or Guardian

Refusal to Share Medical Information

I, _____, do not want to share my child's medical information between Betances School Health Clinic and HHPACC. I understand that my refusal will not keep my child from receiving medical care at either the school clinic or HHPACC and my refusal will not be held against me.

Date: Signature_____
Parent or Guardian

PROHIBITION ON REDISCLOSURE: This information has been disclosed from records whose confidentiality is protected by Federal and State law. Regulations prohibit making any further disclosure of this information except with the specific written consent of the person to whom it pertains. A general authorization for the release of medical or other information if held by another party is NOT sufficient for this purpose. Regulations state that any person who violates any provision of this law shall be fined not more than $500 in the case of the first offense and not more than $5,000 in the case of each subsequent offense.

(Please note: this document has also been translated into Spanish.)

5.4. Sample Recommendations

This sample form should not be used without the advice of the user's legal counsel.

Policy and Procedures: Computerized Medical Records

I. GENERAL PROVISIONS

Purpose

The purpose of this recommended policy is to establish reasonable precautions and policies that attempt to:

1. Balance patients' privacy rights and the confidentiality of Identifiable Patient Information with legitimate data uses;
2. Ensure the accuracy of information contained in patients' medical records;
3. Ensure that parents and legal guardians of patients are adequately informed of:
   a. their right to privacy and confidentiality for their child's Identifiable Patient Information;
   b. their right to personal access to such information;
   c. their right to refuse transfer of information;
   d. their right to revoke consent to transfer of information; and
   e. limits placed on these rights, as required by state or federal laws or regulations.

Definitions

For purposes of this policy, the following definitions apply:

Audit system is a system built into the computer that enables the information security manager to identify who logs into which files and which applications CHN computer users are running.

Authorized personnel are any employees or volunteers of the facility who have signed "User Access and Confidentiality Agreement" and thereby are granted permission to read, retrieve, modify, input or file, and destroy data contained in the medical records systems.

Children's Health Network is a publicly-funded entity that has designed a computer system to link care facilities for pediatric patients in downtown Hartford.

Confidentiality is a form of Privacy characterized by a fiduciary relationship, such as between health care provider and patient. Personal information obtained in the course of such relationship shall not be disclosed by the health care provider unless: 1) the patient's parent or guardian is made aware of and makes an informed consent to the disclosure, or 2) disclosure is otherwise required by state or federal laws or regulations.

Data security means a set of technical and administrative procedures designed to protect medical records systems against unwarranted disclosure and to safeguard the systems themselves.

Data integrity includes methods to ensure that data is entered and changed only in an authorized and prescribed manner, and that random errors do not creep into the data.

Facility means the health care site that will apply this policy.

Identifiable patient information means any information contained in a patient's medical record that facilitates the identification of the patient. Examples include, but are not limited to: name, Social Security number, address, phone number, name of parent(s) or guardian(s), date of birth.

Medical records systems means data stored on either hard copies or on the computer, and involving the medical records of patients at the facility.

Privacy is the right of an individual or an individual's parent, guardian, or authorized representative to limit access by others to information about the individual.

Providers of medical data are the physician and all other members of the health care team who have generated the medical information that is part of the medical records systems. "Provider of medical data" cannot be the facility's clerk. Therefore, the provider of medical data is ultimately responsible to the patients.

Disclaimer of Responsibility

The Children's Health Network is not responsible for data security or the confidentiality of identifiable patient information. The policies contained herein are draft recommendations only. The adoption and implementation of these proposed policies is the responsibility of the facility's management. Additionally, an order to implement these policies, procedures must be delineated at each facility.

Transfer of Data Between Two Medical Sites/Consent

Information from Betances School Health Clinic medical records will be entered into the computer at Betances School Health Clinic to establish a medical database.

No data will be transferred to Hartford Hospital Pediatric Ambulatory Care Clinic (HHPACC) until the parent or guardian gives informed consent and signs a consent form. The signature indicates consent to share information between Betances School Health Clinic and HHPACC. Students whose parents do not sign the consent form will still get medical care at the Betances School Health Clinic and HHPACC, but no data will be transferred to HHPACC.

Consent forms should clearly indicate those areas where reporting is required by Connecticut and federal law. The consent form also states that medical information shared between the sites can include HIV, psychiatric, and drug and alcohol-related information.

Consent forms are renewed every year.

The parents or guardian are informed that they have a right to see a copy of their childÕs medical records.

Consent forms are sent home with children at the beginning of each school year. A system for obtaining informed consent will be in place at each site for those individuals who choose to have information transferred but have never signed the consent form. A copy of an information sheet and consent form is attached.

II. DATA SECURITY

Hard Copies of Medical Records

It is the responsibility of the facility managing the medical record and the computers to maintain policies to keep secure the hard copy medical records generated from the computer and to keep secure the computers themselves.

Computerized Medical Records

1. Data Users' Responsibility for Confidentiality: Authorized personnel are trained in entering data from the medical record hard copies onto the computer network. This includes initial training describing data users' responsibility for confidentiality, periodic review of procedures, and annual review for all individuals who have access to the computer patient record (CPR). Responsibility and confidentiality statements are signed by new employees using the computer, and annually for all authorized personnel. Additionally, a reminder notice is programmed on the computer screen at the beginning of the program indicating the confidential nature of the patient information.

2. Confidentiality of Data: Access to identifiable patient information is limited to authorized personnel a) directly involved in the care of that patient at the facility; b) to individuals or organizations expressly authorized by the patient's parent or guardian; or c) as otherwise required by law.

3. System Access Control: System access control attempts to prevent unauthorized users insofar as is reasonable from logging onto the system. Policies and procedures within the institution will be established for the following:

a. User Access and Confidentiality Agreement: All individuals with access to the computer will sign the User Access and Confidentiality Agreement (attached).

b. Passwords: Authorized personnel are given unique passwords. These are automatically changed every 60-90 days and consist of at least six digits of both numbers and letters. Authorized personnel memorize their passwords.

c. Login attempt limitation: The system limits the number of login attempts and record unsuccessful ones.

d. Password cancellation: Passwords not used for a specific period of time are canceled.

e. User identification codes (user ID) that identify the terminal users and application programs: Access to the system and application shall be denied if the application password and user ID is not listed in the access control file. User IDs also allow the system to report the activities of each individual logged onto the system.

f. Access will be defined by the time of day and day of the week according to the needs of the facility. If not needed, a computer would not be available after hours so that it would not be vulnerable to others using the area.

g. Authorized personnel will be warned not to disclose to or share passwords with any other persons. Any evidence of violation of this policy may be cause for termination of employment with the facility.

h. When any authorized personnel ends employment or volunteering at the facility, the password and user ID for that person will be immediately deactivated.

i. Authorized personnel must log off the computer whenever they finish using it. Whenever any authorized personnel fail to log off at the end of a work day, that person must report to the supervisor in charge of data management the next day before logging on again.

j. Linkage of the data to any computer networks other than the one connecting Betances School Health Clinic and HHPACC is expressly prohibited. Prohibited networks include the Internet.

III. EQUIPMENT SECURITY

It is the responsibility of the facility managing the medical record to maintain policies for the following:

Computers:

Computers will be placed in secure locations in the facility. The room(s) where they are contained will be locked, and the computers themselves locked with keys when not in use. Keys will be kept in a secure location.

Control of Printouts/Disks:

1. Printing of medical records or printouts from computer data will be protected to ensure confidentiality of medical record. Rules will be established for use of printouts.
2. Downloading any CHN data onto portable computer disks is strictly prohibited.

IV. DATA INTEGRITY

It is the responsibility of the facility managing the medical record to maintain policies so that:

1. Facilities will have systems for updating data to ensure confidentiality and accuracy.
2. A system will be set up to ensure accuracy in the transfer of information from the medical record to the computer. Initially all entries will be checked for accuracy, followed by checks of every second, fourth entry, etc. Subsequently, auditing will be done on a regular basis, i.e., monthly.
3. An auditing review system will be set up to review the information from the computer audit system on a regular basis. This may include: a) activities of specific user IDs; b) logins, logouts, and break-in attempts; c) selected uses of files and hardware devices.
4. A system of journaling of all system activities will be set up. This will assist in the auditing system. Activities include any changes made to the on-line data and the dates they were made.

V. RESEARCH REQUESTS

Any requests for data for the purpose of research projects must be requested through the facility's Institutional Review Board (IRB).

VI. INFORMATION SECURITY EDUCATION PROGRAM

An information security education program will be developed to enhance the security awareness of CHN computer users to improve their information security practices, and to protect patient confidentiality.

5.5. Sample Form

This sample form should not be used without the advice of the user's legal counsel.

CHILDREN'S HEALTH NETWORK (CHN)
USER ACCESS AND CONFIDENTIALITY AGREEMENT

I, _____, _____
(Print Name) (Social Security Number)

request permission for access to the CHILDREN'S HEALTH NETWORK (CHN). CHN contains CONFIDENTIAL medical information. I have read and discussed the policies and procedures for using the CHN computer system and I will comply with these policies and procedures including:

- Conforming to the privileges of use granted to me to read, edit, and/or copy records and not to exceed these privileges. Also using equipment, programs and data according to the rights granted and during time periods specified;
- Accessing only that information which I have a need to know in the course of my work at the Betances School Clinic or Hartford Hospital Pediatric Ambulatory Care Clinic (HHPACC);
- Assuring that identifiable information contained in the CHN network will not be disclosed to any individual or agency not specifically authorized by the consent form of a particular child;
- Taking appropriate security precautions to prevent the examination or copying of any written documents by unauthorized individuals, and additionally not examining or copying any written document except as properly authorized within the scope of my employment;
- Protecting the restricted use of my user logon and password and not disclosing it, sharing it with, or transferring it to another. I will also not write my user logon or password down in an unsecured location where unauthorized individuals might have access to it;
- Keeping the Computer hardware and software secure according to policies and procedures established by my facility;
- Signing off the computer screen when I am no longer using it.

I recognize my responsibility to hold medical information in confidence and to adhere to the proper operating policies and procedures when using the CHILDREN'S HEALTH NETWORK (CHN). Further, I understand that any violation of the confidentiality of medical information may result in disciplinary action.

Signature_____ Date_____

Signature_____ Date_____
Immediate Supervisor

__ APPROVED USER ID_____ Date_____

Acronym Glossary

AMA:	American Medical Association
CCMC-PMC:	Connecticut Children's Medical Center - Primary Care Clinic
CHN:	Children's Health Network
CPRI:	Computerized Patient Records Institute
HHPACC:	Hartford Hospital Pediatric Ambulatory Care Clinic
HPCC:	Hartford Primary Care Consortium
HRSA:	Health Resources and Services Administration
JCAHO:	Joint Commission on Accreditation of Health Organizations
MCHB:	Maternal and Child Health Bureau, PHS
SPRANS:	Special Programs of Regional and National Significance